EC-Council

CHFI Exam Blueprint v2.1

Domains	Objectives	Weightage	Number of Questions
1. Forensic Science	• Computer Forensics Objective and Need • Forensics Readiness • Cyber Crime • Web Applications and Webservers Attacks • Email Crimes • Network Attacks • Forensics on Mobile Devices • Cyber Crime Investigation • Computer Forensics Investigation Methodology • Reporting a Cyber Crime • Expert Witness	15%	22
2. Regulations, Policies and Ethics	• Searching and Seizing Computers with and without a Warrant • Laws and Acts against Email Crimes • Laws pertaining to Log Management • Policies Pertaining to Mobile Forensics • Laws and Acts against Email Crimes • General Ethics While Testifying	10%	15
3. Digital Evidence	• Digital Evidence • Types of Digital Evidence • Rules of Evidence • Electronic Evidence: Types and Collecting Potential Evidence • Electronic Crime and Digital Evidence Consideration by Crime Category • Computer Forensics Lab • Understanding Hard Disks • Disk Partitions and Boot Process • Understanding File Systems • Windows File Systems • Linux File Systems • Mac OS X File Systems • RAID Storage System • File Carving • Image Files • Analyze Logs • Database Forensics • Email Headers • Analyzing Email headers • Malware Analysis • Mobile Operating Systems	20%	30

4. Procedures and Methodology	• Investigating Computer Crime • Computer Forensics Investigation Methodology • Digital Evidence Examination Process • Encryption • First Responder • First Response Basics • Roles of First Responder • Data Acquisition and Duplication • Defeating Anti-forensics Techniques • Log Management and Event Correlation • Network Forensics (Intrusion Detection Systems (IDS)) • Computer Forensics Reports and Investigative Report Writing	20%	30
5. Digital Forensics	• Recover Data • File System Analysis • Windows Forensics • Linux Forensics • MAC Forensics • Recovering the Deleted Files and Partitions • Steganography and Image File Forensics • Steganalysis • Application Password Crackers • Investigating and Analyzing Logs • Investigating Network Traffic • Investigating Wireless Attacks • Web Attack Investigation • Investigating Email Crime and Violation • Mobile Forensic Process • Cloud Forensics • Malware Forensics • Defeating Anti-Forensic Techniques	25%	37
6. Tools/Systems/ Programs	• First Responder Toolkit • Windows Forensic Tools (Helix3 Pro, X-Ways Forensics, Windows Forensic Toolchest (WFT), Autopsy, The Sleuth Kit (TSK), etc.) • Data Acquisition Software Tools UltraKit Forensic Falcon, etc.) • Tools to defeat Anti-Forensics • Steganography Tools • Database Forensics Tools • Password Cracking Tools • Network Forensics Tools • Web Security Tools, Firewalls, Log Viewers, and Web Attack Investigation Tools • Cloud Forensics Tools • Malware Forensics Tools • Email Forensics Tools • Mobile Forensics Software and Hardware Tools • Report Writing Tools	10%	16